

# Firepower Threat Defense(FTD)で実行されているアクティブなSnortバージョンの判別

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[FTDで稼働しているアクティブなSnortバージョンの確認](#)

[FTDコマンドラインインターフェイス\(CLI\)](#)

[Cisco FDMによるFTDの管理](#)

[Cisco FMCで管理されるFTD](#)

[Cisco CDOによるFTD管理](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Cisco FDM、Cisco FMC、またはCDOによってCisco FTDが管理されている場合に、Cisco FTDが実行するアクティブなSnortバージョンを確認する手順について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco Firepower Management Center ( FMC )
- Cisco Firepower Threat Defense ( FTD )
- Cisco Firepower Device Manager ( FDM )
- Cisco Defense Orchestrator(CDO)

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Firepower Threat Defense v6.7.0および7.0.0
- Cisco Firepower Management Center v6.7.0および7.0.0
- Cisco Defense Orchestrator

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

SNORT® Intrusion Prevention System (IPS ; 侵入防御システム) は正式に Snort 3 をリリースしました。これは包括的なアップグレードで、パフォーマンスの強化、処理速度の高速化、ネットワークのスケラビリティの向上、および200を超えるプラグインの範囲を実現し、ネットワークのカスタムセットアップを作成できます。

Snort 3 の利点には次のようなものがあります。

- パフォーマンスの向上
- SMBv2 インспекションの向上
- 新しいスクリプト検出機能
- HTTP/2 インспекション
- カスタムルールグループ
- カスタム侵入ルールを記述しやすくする構文。
- インラインの結果が侵入イベントでドロップされる理由。
- VDB、SSL ポリシー、カスタムアプリケーションディテクタ、キャプティブポータルIDソース、および TLS サーバID ディスカバリに変更が導入されると、Snort は再起動しません。
- サービスアビリティの向上 : Snort 3 固有のテレメトリデータが Cisco Success Network に送信され、ログのトラブルシューティングが向上します。

Snort 3.0 のサポートは、Cisco Firepower Threat Defense (FTD) が Cisco Firepower Device Manager (FDM) で管理されている場合に、6.7.0 で導入されました。

---

 注:FDMで管理される新しい6.7.0 FTD展開では、Snort 3.0がデフォルトのインспекションエンジンです。古いリリースから6.7にFTDをアップグレードすると、Snort 2.0がアクティブインспекションエンジンとして残りますが、Snort 3.0に切り替えることもできます。

---

 注 : このリリースのSnort 3.0では、仮想ルータ、時間ベースのアクセス制御ルール、または TLS 1.1以前の接続の復号化はサポートされていません。Snort 3.0は、これらの機能が不要な場合にのみ有効にしてください。

---

次に、Firepowerバージョン7.0では、Cisco FDMとCisco Firepower Management Center(FMC)の両方で管理されるFirepower Threat Defense(FTD)デバイスに対するSnort 3.0のサポートが導入されました。

---

 注：新しい7.0 FTD導入では、Snort 3がデフォルトのインスペクションエンジンになっています。アップグレードされた導入は引き続きSnort 2を使用しますが、いつでも切り替えることができます。

---

 注意:Snort 2.0と3.0は自由に切り替えできるので、必要に応じて変更を元に戻すことができます。バージョンを切り替えるたびにトラフィックが中断されます。

---

 注意: Snort 3に切り替える前に、『[Firepower Management Center Snort 3コンフィギュレーションガイド](#)』を読んで理解しておくことを強くお勧めします。機能の制限と移行手順に特に注意してください。Snort 3へのアップグレードは影響を最小限に抑えるように設計されていますが、機能が正確にマッピングされるわけではありません。アップグレード前の計画と準備は、トラフィックが期待どおりに処理されることを確認するのに役立ちます。

---

## FTDで稼働しているアクティブなSnortバージョンの確認

### FTDコマンドラインインターフェイス(CLI)

FTDで実行されているアクティブなSnortのバージョンを確認するには、FTD CLIにログインして、`show snort3 status`コマンドを実行します。

例1：出力が表示されない場合、FTDはSnort 2を実行します。

```
<#root>
>
show snort3 status
>
```

例2：出力に「Currently running Snort 2」と表示されている場合、FTDはSnort 2を実行しています。

```
<#root>
>
show snort3 status
```

```
Currently running Snort 2
```

例3：出力に「Currently running Snort 3」と表示されている場合、FTDはSnort 3を実行しています。

```
<#root>
```

```
>
```

```
show snort3 status
```

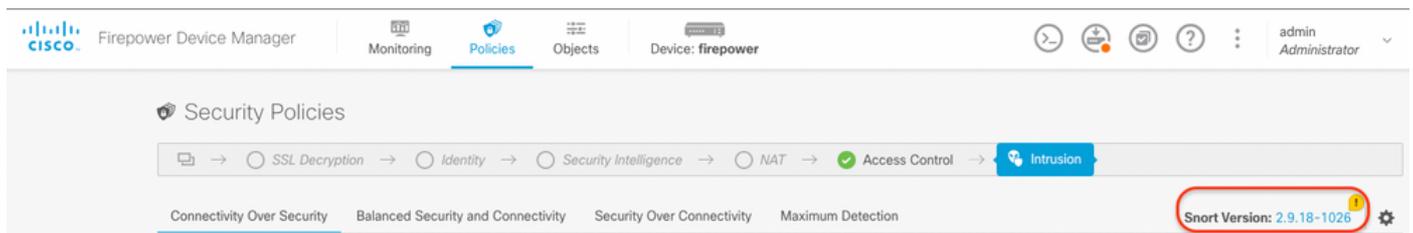
Currently running Snort 3

## Cisco FDMによるFTDの管理

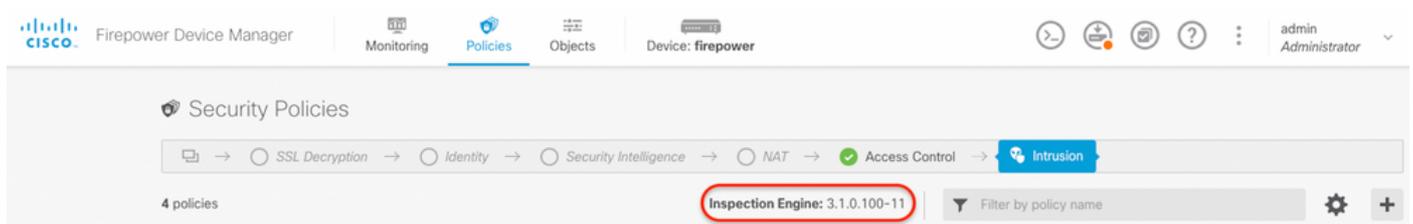
Cisco FDMによって管理されているFTDで実行されているアクティブなSnortのバージョンを確認するには、次の手順を実行します。

1. FDM WebインターフェイスからCisco FTDにログインします。
2. メインメニューからPoliciesを選択します。
3. 次にIntrusionタブを選択します。
4. Snortのバージョンまたは「インスペクションエンジン」セクションを探して、FTDでアクティブなSnortのバージョンを確認します。

例1:FTDがSnortバージョン2を実行している。



例2:FTDがSnortバージョン3を実行している。



## Cisco FMCによって管理されるFTD

Cisco FMCによって管理されているFTDで実行されているアクティブなSnortのバージョンを確認するには、次の手順に従います。

1. Cisco FMC Webインターフェイスにログインします。
2. DevicesメニューからDevice Managementを選択します。
3. 次に、適切なFTDデバイスを選択します。
4. [編集 ( Edit ) ] アイコン ( 鉛筆の形 ) をクリックします。
5. Deviceタブを選択し、Inspection Engineセクションを探して、FTDでアクティブなSnortのバージョンを確認します。

## 例1:FTDがSnortバージョン2を実行している。

The screenshot shows the Cisco Firepower Management Center interface for device vFTD-1. The 'Inspection Engine' section is highlighted with a red box and shows 'Snort 2' is selected. A 'NEW Upgrade' notification is present, indicating that Snort 3 is available and offers performance and security improvements. The notification includes a warning that switching versions requires a deployment and may cause traffic loss.

Section	Parameter	Value
General	Name	vFTD-1
	Transfer Packets	Yes
	Mode	Routed
	Compliance Mode	None
	TLS Crypto Acceleration	Disabled
License	Performance Tier	FTDv - Variable
	Base	Yes
	Export-Controlled Features	Yes
	Malware	Yes
	Threat	Yes
	URL Filtering	Yes
	AnyConnect Apex	No
	AnyConnect Plus	No
	AnyConnect VPN Only	No
	System	Model
Serial		[Redacted]
Time		2023-04-20 00:57:11
Time Zone		UTC (UTC+0:00)
Version		7.0.4
Management	Host	[Redacted]
	FMC Access Interface	Management Interface

## 例2:FTDがSnortバージョン3を実行している。

The screenshot shows the Cisco Firepower Management Center interface for device FTD1010-1. The 'Inspection Engine' section is highlighted with a red box and shows 'Snort 3' is selected. A 'Revert to Snort 2' button is visible, indicating that Snort 2 was previously used. The notification about Snort 3 improvements is also present.

Section	Parameter	Value	
General	Name	FTD1010-1	
	Transfer Packets	Yes	
	Mode	Routed	
	Compliance Mode	None	
	TLS Crypto Acceleration	Disabled	
License	Base	Yes	
	Export-Controlled Features	Yes	
	Malware	Yes	
	Threat	Yes	
	URL Filtering	Yes	
	AnyConnect Apex	Yes	
	AnyConnect Plus	Yes	
	AnyConnect VPN Only	No	
	System	Model	Cisco Firepower 1010 Threat Defense
		Serial	[Redacted]
Time		2023-04-20 01:44:01	
Time Zone		UTC (UTC+0:00)	
Version		7.0.4	
Management	Host	[Redacted]	
	FMC Access Interface	Management Interface	

## Cisco CDOによって管理されるFTD

Cisco Defense Orchestratorによって管理されているFTDで実行されているアクティブなSnortの

バージョンを確認するには、次の手順に進みます。

1. Cisco Defense Orchestrator Web インターフェイスにログインします。
2. Inventoryメニューから、適切なFTDデバイスを選択します。
3. Device Detailsセクションで、Snort Versionを探します。

例1:FTDがSnortバージョン2を実行している。

The screenshot shows the Cisco Defense Orchestrator (CDO) Inventory page. The left sidebar contains a navigation menu with options like Dashboard, Inventory, Policies, Objects, VPN, Analytics, Change Log, Jobs, Tools & Services, and Settings. The main area displays a table of FTD devices. The first device, 'FTDv', is selected and highlighted. Its configuration status is 'Synced' and its connectivity is 'Online'. The right-hand 'Device Details' panel shows various attributes: Location (n/a), Model (Cisco Firepower Threat Defense for Azure), Serial (redacted), Version (7.2.0), Onboarding (Registration Key), and Method (redacted). The 'Snort Version' is highlighted with a red box and shows the value '2.9.21-102'. Below this, a 'Synced' status is confirmed with the message 'Your device's configuration is up-to-date.' and a 'Device Actions' menu with options like 'Check for Changes', 'Manage Licenses', 'Workflows', and 'Remove'.

例2:FTDがSnortバージョン3を実行している。

This screenshot is similar to the first one, showing the CDO Inventory page. In this instance, the configuration status for the selected 'FTDv' device is 'Not Synced'. The 'Device Details' panel on the right shows the 'Snort Version' as '3.1.211-126', which is also highlighted with a red box. Below this, a 'Not Synced' status is indicated with the message: 'The configuration has been modified in FMC. Synchronize your device's configuration by deploying the changes from FMC Deployment page.' The 'Device Actions' menu remains the same as in the first screenshot.

## 関連情報

- [Cisco Firepowerリリースノート、バージョン6.7.0](#)
- [Cisco Firepowerリリースノート、バージョン7.0](#)
- [Snort 3のWebサイト](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。